Michael Kind, Esq.
Nevada Bar No.: 13903
KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123
(702) 337-2322
(702) 329-5881 (fax)
mk@kindlaw.com

George Haines, Esq.
Nevada Bar No.: 9411
Gerardo Avalos, Esq.
Nevada Bar No.: 15171
FREEDOM LAW FIRM, LLC
8985 S. Eastern Ave., Suite 350
Henderson, NV 89123
(702) 880-5554
(702) 385-5518 (fax)
Attorney for Plaintiff Jehu Bryant,
and on behalf of all others similarly situated

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

Jehu Bryant, individually and on behalf of all others similarly situated,

Plaintiff,

v.

MX Holdings US, Inc., CFP Fire Protection, Inc., COSCO Fire Protection, Inc., and Firetrol Protection Systems, Inc.,

Defendants.

Case No.: 2:22-cv-00855-GMN-EJY

Response in opposition to Defendants' motion to dismiss [ECF No. 17]

Jehu Bryant ("Plaintiff") hereby submits his response in opposition to Defendants' motion to dismiss, ECF No. 17.

This response is based upon the accompanying memorandum of points and authorities, all papers and records on file herein and on such oral arguments which may be presented at the hearing of the motion.

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

Memorandum of Points and Authorities

I. Introduction

Plaintiff respectfully requests that this Court deny Defendants' motion.

First, Article III standing exists. Where a plaintiff alleges that there is a "substantial risk of identity theft" because of a data breach, there is an injury-in-fact. *In re Zappos.com, Inc.*, 888 F.3d 1020 (9th Cir. 2018); *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010). Plaintiff also alleged other injuries-in-fact, including the lost value in his personal information, invasion of privacy, mitigation costs, and lost time. Courts recognize these harms as injuries-in-fact in similar cases.

Defendants' nine months delay to notify Plaintiff of the breach exacerbated these harms. These harms are directly traceable to Defendants' conduct and misconduct in failing to keep Plaintiff's information secure. Plaintiff injuries are redressable through money damages and injunctive relief.

Second, as evidenced by public record filings with California's Attorney General, diversity jurisdiction is established under CAFA because more than 100 people were impacted. Also, after a review of the outcome in similar cases, the amount in controversy is well over $5,000,000. Defendant fails to raise any dispute on these issues. But, in any case, jurisdictional discovery will resolve the issue.

Third, Plaintiff's claims are adequately pleaded. As to Plaintiff's negligence claim, an employer has a duty of care to secure its employees' information. Defendants' breach proximately caused Plaintiff's injuries: a substantial risk of fraud, loss of value of personal information, monitoring costs, lost time, invasion of privacy, and emotional harm. Such harms give rise to a negligence claim.

The economic loss rule does not apply because Plaintiff sustained non-economic damages and because the doctrine does not apply where the parties have an employer-employee special relationship. Numerous courts have recognized this.

Next, Plaintiff's invasion of privacy claim is well pleaded. Invasion of privacy claims have routinely survived motions to dismiss where, as here, the data breach involved medical information. The disclosure of such information constitutes an "egregious breach of the social norms" that is "highly offensive."

Plaintiff also properly pleaded his contract claims. The case law supports that a breach of contract claim exists when a company fails to protect its employees' private information. Defendants promised to safeguard Plaintiff's data, that he was required to provide his employer. Defendants do not cite any on-point cases.

Finally, Plaintiff has stated a claim for declaratory and injunctive relief. Plaintiff's and the putative class members' private information is still in Defendants' unsecure systems. He is still at risk of attack by criminals. Plaintiff seeks relief to prevent further harm.

II. Statement of the facts

Defendants offer fire protection services.[1] Plaintiff is a former employee of Defendants. As a condition of employment, Plaintiff was required to provide his personal information to Defendants. Defendants, in turn, assured Plaintiff that they will keep his information secure. ECF No. 1, ¶¶ 63-72.

On or around May 10, 2022, Plaintiff, and thousands of other employees and former employees of Defendants, were sent letters from Defendants notifying them of a data breach that happened in August 2021. Compl., ECF No. 1, ¶ 4. Around the same time, Defendants submitted their data breach notification to the California Attorney General's office. Attorney general, *Submitted Breach Notification Sample*,

[1] Cosco and Firetrol are fire protection companies. *See Rd. Sprinkler Fitters Local Union No. 669*, U.A. v. NLRB, Nos. 17-1159, 17-1182, 2018 U.S. App. LEXIS 15270, at *3 (D.C. Cir. June 1, 2018). CFP is a fire protection subcontractor. *Id.* The three companies are wholly owned subsidiaries of MX Holdings. *Id.*

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

available at https://oag.ca.gov/ecrime/databreach/reports/sb24-553265 (last visited August 24, 2022).[2]

Plaintiff's name, date of birth, social security number, driver's license number, passport number, financial account numbers, and medical information ("PII") was exposed. *Id.* at ¶ 5. The information was targeted by criminals and is likely for sale on the dark web. *Id.* at ¶ 30. Like other people whose information is obtained by criminals, Plaintiff is at a higher risk of identity theft and fraud. *E.g.*, *Id.* at ¶ 34. Criminals may easily pose as Defendants, law enforcement, or other entity to trick Plaintiff into providing even more personal information. *Id.* at ¶ 33. Thus, even if only some of Plaintiff's information was leaked in the breach, criminals could use that information to access additional information to defraud Plaintiff. *See Id.*

In addition to identity theft and fraud, Plaintiff faces other harms, including credit monitoring costs, identity theft insurance, lost time, anxiety, emotional distress, and a loss of his privacy. *Id.* at ¶ 34. Plaintiff seeks damages injunctive relief to redress these harms. Also, Plaintiff's information is still in Defendants' unsecure systems. Plaintiff seeks additional injunctive relief to prevent future harms.

To seek redress, Plaintiff filed his complaint on May 27, 2022, claiming negligence, invasion of privacy, and breach of contract and implied contract. ECF No. 1. Defendants filed their motion to dismiss on July 29, 2022. ECF No. 17.

III. Legal Standard

In considering a motion to dismiss, "all well-pleaded allegations of material fact are taken as true and construed in a light most favorable to the non-moving party." *E.g.*, *In Re Wal-Mart Wage and Hour Employment Practices*, 490 F. Supp.

[2] Plaintiff received the version of the data breach notice that was sent to those people whose social security number was exposed. *E.g.*, Compl., ECF No. 1, ¶ 5.

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

2d 1091 (D. Nev. 2007) (*citing Wyler Summit P'ship v. Turner Broad. Sys., Inc.*, 135 F.3d 658, 661 (9th Cir. 1998) (citation omitted). There is a strong presumption against dismissing an action for failure to state a claim. *See*, *e.g.*, *Gilligan v. Jamco Dev. Corp.*, 108 F.3d 246, 249 (9th Cir. 1997) (citation omitted). The issue is not whether the plaintiff ultimately will prevail, but whether she may offer evidence in support of her claims. *See Id*. (quoting *Scheuer v. Rhodes*, 416 U.S. 232, 236 (1974)).

It is improper to dismiss a complaint for failure to state a claim if the plaintiff has alleged "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570, 127 S. Ct. 1955, 167 L. Ed. 2d 929 (2007). A claim is plausible on its face when the facts in the complaint allow the court to reasonably infer that the defendant is liable. *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S. Ct. 1937, 173 L. Ed. 2d 868 (2009).

IV. Argument

Defendants' motion should be denied because: (1) Article III standing exists; (2) diversity jurisdiction is established; and (3) Plaintiff's claims are well pleaded.

A. Article III standing is established

Standing exists because Plaintiff: (1) suffered an injury in fact; (2) that is traceable to Defendants' conduct; and (3) that can be redressed in this case.

1. Plaintiff plausibly pleaded an injury in fact

Plaintiff's injuries include: (1) an increased, and substantial, risk of identity theft; (2) a loss of value in his PII; and (3) mitigation costs. Furthermore, (4) these injuries were exacerbated because of the Defendants' delay in giving notice.

a. Plaintiff plausibly pleaded a substantial risk of identity theft or fraud

The authority in the Ninth Circuit is plain: the risk of identity theft or fraud is sufficient to support Article III standing. *Zappos*, 888 F.3d at 1028 ("The sensitivity of the personal information, combined with its theft [meant] that the plaintiffs had adequately alleged an injury in fact supporting standing."); *Krottner*, 628 F.3d 1139

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

(where there is a substantial risk of identity theft, injury-in-fact is satisfied); *see also In re Yahoo! Inc., Customer Data Sec. Breach Litig.*, No. 16-MD-02752-KHK, 2017 WL 3727318, *12-13 (N.D. Cal. Aug. 30, 2017) (plaintiffs successfully alleged a concrete and imminent threat of future harm for Article III standing); *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1214-15 (N.D. Cal. 2014) (finding Article III standing where a third party could engage in future identity theft).

The hackers breached Defendants' system to commit fraud and identity theft. "Why else would hackers . . . steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Zappos*, 888 F.3d at 1026 n. 6 (quoting *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015)).

Here, Plaintiff's PII, including his social security number, like in *Krottner*, was obtained by cybercriminals. *E.g.*, Compl., ECF No. 1, ¶¶ 25, 27; 625 F.3d at 1140. This gives rise to a "substantial risk of identity theft," an "injury-in-fact."

Importantly, Plaintiff does not need to allege that his PII was misused. "Plaintiffs . . . whose personal information has been stolen but not misused, have suffered an injury sufficient to confer standing." *Krottner*, 628 F.3d at 1140; *Walter v. Kimpton Hotel & Rest. Grp., LLC*, No. 16-cv-05387-VC, 2017 WL 1398660, at *1 (N.D. Cal. Apr. 13, 2017) (It is not necessary to "actually suffer the misuse of his data or an unauthorized charge before he has an injury for standing purposes."). Here, Plaintiff's driver's license number, social security number, and other PII was breached and is likely for sale on the dark web. Compl., ECF No. 1, ¶ 30. Plaintiff's PII was stolen by criminals from Defendants' computers. Article III standing exists.

The case law relied on by Defendants is inapplicable

Defendants are mistaken in their reliance on *Stasi v. Immediata Health Group Corp.*, 2020 WL 2126317, *5-6 (S.D. Cal. 2020). In that case, the court distinguished *Zappos* and *Krottner* because no credit card number or social security number were

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

at issue. *Stasi* also found the fact that the PII was stolen or hacked by criminals in *Zappos* and *Krottner* was dispositive. *Id. Stasi* is therefore inapplicable in this case, because like *Zappos and Krottner*, Plaintiff's social security number was breached.

Similarly, *Travis v. Assured Imaging LLC*, No. CV-20-00390-TUC-JCH, 2021 U.S. Dist. LEXIS 89129, at *3 (D. Ariz. May 10, 2021) does not apply. In that case, "The investigation was unable to determine the full extent of information that was accessed by the unknown actor." *Id.* Here, the hacker actually accessed the records that contained Plaintiff's PII. *E.g.*, Comp., ECF No. 1, ¶ 26.

Jackson v. Loews Hotels, Inc., No. ED CV 18-827-DMG (JCx), 2019 U.S. Dist. LEXIS 124525, at *11 (C.D. Cal. July 24, 2019) is easily distinguishable. In that case, the plaintiff "closed or modified her accounts to mitigate the impact of the data breach, [so] has not established a certainly impending future injury sufficient to confer standing." *Id.* No such claims could be made here where Plaintiff's social security number, driver's license information, and medical history, among other things, were exposed in the hack—sensitive PII that cannot be closed or modified.

Finally, *TransUnion LLC v. Ramirez*, 141 S.Ct. 2190 (2021) actually supports Plaintiff's position. Under *Ramirez*, where defamatory credit reports were sent to third-party businesses, the Court had "no trouble concluding that the [] class members suffered a concrete harm that qualifies as an injury in fact." *Id.* at 2209. Here, Plaintiff's PII was accessed from Defendants' computers by criminals, making this case directly analogous to *Ramirez* wherein the Court found standing. *Id.* Defendants cite portions that relate only to people whose information was not disclosed. Mot., ECF No. 17, p. 8. Plaintiff's PII was disclosed to others. Therefore, *Ramirez* supports Plaintiff's position. *E.g.*, *Wynne v. Audi of Am.*, No. 21-cv-08518-DMR, 2022 U.S. Dist. LEXIS 131625, at *14 (N.D. Cal. July 25, 2022) (discussing *Ramirez* at length and concluding that the invasion of the "right to privacy [] constitutes a concrete harm" in data breach case).

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

Plaintiff faces a substantial risk of identity theft. Article III standing exists.

b. Plaintiff sufficiently pleaded a loss of value of PII

Plaintiff also lost value in his PII, an injury-in-fact. *In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-LHK, 2016 WL 3029783, at *15, *25 (N.D. Cal. May 27, 2016) (*Anthem II*) ("Plaintiffs have also sufficiently pleaded damages for Loss of Value of PII . . . . [T]he Ninth Circuit and a number of district courts have approved such damages theories . . . . '[P]laintiffs alleged that the information disclosed [could] be used to obtain personal information about plaintiffs, and that they were harmed both by the dissemination of their personal information and by losing the sales value of that information.'") (quoting *In re Facebook Privacy Litig.*, 572 Fed. Appx. 494, 494 (9th Cir. 2014)).

Plaintiff adequately alleged the value of his PII and the implications of such PII in the hands of cybercriminals. Compl., ECF No. 1, ¶¶ 18-37, 71, 85. These allegations more than suffice to support Loss of Value of PII as an injury-in-fact under the controlling law.

c. Plaintiff sufficiently pleaded out-of-pocket monitoring costs, lost time, and other non-economic harms

Plaintiff suffered mitigating costs, lost time, and other harms that amount to cognizable injuries-in-fact. "[C]ourts have held similar allegations of out of pocket expenses sufficient to establish standing." *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2017 U.S. Dist. LEXIS 140212, at *93 (N.D. Cal. Aug. 30, 2017) ("In order to establish standing for a UCL claim, Plaintiffs must show that they personally lost money or property as a result of the unfair competition.") (quotations omitted); *see also Adobe*, 66 F. Supp. 3d at 1207 (standing existed where the plaintiff alleged costs of monitoring).

Additionally, in data breach cases, the loss of time establishes injury in fact. "[L]oss of time establishes injury in fact." *Bass v. Facebook, Inc.*, 394 F. Supp. 3d

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

1024, 1035 (N.D. Cal. 2019) (citing *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 828 (7th Cir. 2018)); *Yahoo!*, *at* *71-72 (where a plaintiff was "required to spend significant time and effort monitoring these charges and mitigating their fall out," standing exists); *Adkins v. Facebook, Inc*., 424 F. Supp. 3d 686, 692 (N.D. Cal. 2019) ("The time lost by plaintiff establishes a harm for standing purposes."); *Huynh v. Quora, Inc.*, No. 18-cv-07597-BLF, 2019 U.S. Dist. LEXIS 235733, at *16 (N.D. Cal. Dec. 19, 2019) ("Plaintiffs have established standing through the dual harms of increased risk of future harm and loss of time."); *see also Stasi*, 501 F. Supp. 3d at 918 ("Accordingly, at this early stage in litigation, Plaintiffs allege plausible damages in the form of lost time.").

Here, Plaintiff adequately alleged out-of-pocket monitoring costs, lost time, psychological damages, and a loss of his privacy. *E.g.*, Compl., ECF No. 1, ¶56. Therefore, Plaintiff has stated a cognizable injury-in-fact.

d. Plaintiff sufficiently pleaded additional harm related to the delayed notice

Defendants' delay of nine months to notify Plaintiff caused him additional harm. A delay of notice creates an incrementally increased risk because of an inability to start mitigative steps. *E.g.*, *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig*., No. 3:19-cv-2284-H-KSC, 2020 U.S. Dist. LEXIS 80736, at *24 (S.D. Cal. May 7, 2020) ("Plaintiffs have adequately alleged incremental harm as a result of Solara's five-month delay in notification.") (citing *Yahoo!*). Here, Plaintiff was therefore injured by being subjected to an increase of risk of fraud based on the Defendants' delay in giving the data breach notice. *E.g.*, Compl., ECF No. 1, ¶¶ 2, 3, 4, 9. Plaintiff suffered an injury-in-fact.

2. Plaintiff adequately pleaded a traceable injury

Plaintiff alleged a traceable connection between Defendants' conduct and his injuries. In data breach cases, standing exists where a plaintiff has alleged a logical connection between the breach and the harm suffered. *Yahoo*, 2017 WL 3727318, at

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

*17 (conferring standing because plaintiffs alleged a "causal chain" of events that linked the defendant's security measures with the specific harms alleged by the plaintiffs); *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp.3d 953, 987 (N.D. Cal. 2016) (finding that the complaint sufficiently established a logical connection between the data breach and the harm alleged by the plaintiffs) (*Anthem I*).

Here, as discussed, Plaintiff's injuries were directly caused by Defendants' conduct that led to the data breach, as in *Yahoo* and *Anthem I.*

Defendants' reliance on *Antman v. Uber Techs., Inc*., No. 15-cv-01175-LB, 2018 U.S. Dist. LEXIS 79371, at *26 (N.D. Cal. May 10, 2018) is misplaced. There, the court specifically distinguished *Zappos* and *Krottner* where, like here, the plaintiffs' social security numbers were exposed, creating a traceable injury.

Wash. Envtl. Council v. Bellon, 732 F.3d 1131, 1138 (9th Cir. 2013), relied on by Defendants, is distinct. That case involved conservation groups' claims against government agencies over greenhouse gas emissions. The case is inapplicable.

Defendant mis-quotes *In re Uber Techs., Inc., Data Sec. Breach Litig.*, No. CV182970PSGGJSX, 2019 WL 6522843, at *5 (C.D. Cal. Aug. 19, 2019). Mot., ECF No. 17, p. 11:3. That case only involved a motion to compel arbitration.

Instead, this Court should follow *Zappos*, and find that Plaintiff has established traceability: "Plaintiffs sufficiently allege that the risk of future harm they face is 'fairly traceable.'" *Id.* (citation and quotations omitted).

3. Plaintiff adequately pleaded redressability by a favorable decision

Plaintiff sufficiently alleged that his injuries are redressable by a favorable ruling, both through money damages and injunctive relief.

If he prevails, a jury could award damages for Plaintiff's claims. Damages are available in data breach cases. *Zappos*, 888 F.3d at 1030 ("If Plaintiffs succeed on the merits, any proven injury could be compensated through damages."); *Anthem II*, 2016 WL 3029783, at *15; *Yahoo*, 2017 WL 3727318, at *12-13; *Adobe*, 66 F. Supp.

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

3d at 1214-15; *see Calhoun v. Google LLC*, No. 20-CV-05146-LHK, 2021 WL 1056532, at *21 (N.D. Cal. Mar. 17, 2021) ("[C]ourts have recognized the 'growing trend ... to recognize the lost property value' of personal information"); *In re Experian Data Breach Litig.*, No. SACV151592AGDFMX, 2016 WL 7973595, at *5 (C.D. Cal. Dec. 29, 2016) ("[A] growing number of federal courts have now recognized Loss of Value of PI as a viable damages theory."); *Facebook*, 572 F. App'x at 494 (the dissemination, and lost the value, of personal information, gives rise to damages for a breach of contract claim); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) (A court should not "ignore . . . the value that personally identifying information has in our increasingly digital economy."); *see also Galaria*, 663 F. App'x at 388 (where the plaintiffs' sensitive personal information had been stolen by hackers, the "allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs," were sufficiently pleaded). Here, Plaintiff's injuries are redressable through an award of damages.

Next, Plaintiff satisfies redressability by a favorable decision since he seeks injunctive relief. *Zappos*, 888 F.3d at 1030 ("The injury from the risk of identity theft is also redressable by . . . injunctive relief [that] would limit the extent of the threatened injury by helping Plaintiffs to monitor their credit."). Here, Plaintiff seeks, among other things, injunctive relief, including for credit monitoring, identity theft insurance, and for Defendants to implement adequate security protocols. *See* Compl., ECF No. 1, ¶ 88. This would redress the harms caused by Defendants, by protecting him from identity theft, fraud and prevent further harms.

B. Diversity jurisdiction exists under CAFA

Defendants' motion should be denied because: (1) more than 100 people were impacted and the aggregate amount in controversy is well over $5,000,000; and (2) even if not already established, jurisdictional discovery will resolve the issue.

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

1. Jurisdiction exists under section 1332(d) because more than 100 people were impacted and the aggregate amount in controversy is well over $5,000,000

The only relevant facts presently before this Court—Plaintiff's allegations—confirms that more than 100 people were affected. In his complaint, Plaintiff adequately alleged that he, and "thousands" of others were affected by Defendants' data breach. Compl., ECF No. 1, ¶¶ 26, 42. Unless Defendants can show otherwise (and they cannot), the issue, at least at this stage of this case, is not in dispute.

Jurisdictional facts are not in dispute when both parties rely entirely on the plaintiff's complaint. *E.g.*, *Hoffman v. Nat. Factors Nutritional Prods*., No. 12-7244-ES-SCM, 2013 U.S. Dist. LEXIS 140931, at *8 (D.N.J. Aug. 27, 2013) ("The parties disagree as to whether the jurisdictional amount has been met, however, Defendant's notice of removal is premised entirely on factual allegations and legal claims taken from Plaintiff's complaint, and therefore jurisdictional facts are not expressly in dispute between the parties for the purpose of determining CAFA jurisdiction."); *see generally Jones v. ADT Sec. Servs*., No. CV 11-7750 PSG (JCGx), 2012 U.S. Dist. LEXIS 558, at *7 (C.D. Cal. Jan. 3, 2012) (discussing burdens of proof in removal actions). Here, although given the opportunity, Defendants fail to raise any meaningful dispute as to the amount of people affected by the breach.

Notably, Defendant submitted its data breach notification to the California Attorney General, indicating that more than 500 California residents were impacted. In California, there is a requirement to submit a copy of a data breach notification to the Attorney General only when more than 500 California residents are impacted by the breach. *See* California Civ. Code s. 1798.82(f).

Here, it is public record that Defendants submitted their data breach notification to California's Attorney General. Attorney General, *Submitted Breach Notification Sample*, available at https://oag.ca.gov/ecrime/databreach/reports/sb24-

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

553265 (last visited August 24, 2022). Defendants' filing supports that over 500 people were impacted in California alone, sufficient to confer CAFA jurisdiction.

Next, the amount in controversy is more than $5,000,000. The recovery in this case is expected to greatly exceed this threshold, as is common in data breach class actions. For example, Capital One settled for $190 million; Home Depot settled for $192.2 million; Yahoo! Settled for $117.5 million; Uber paid $148 million; Morgan Stanley settled for $120 Million. *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2020 U.S. Dist. LEXIS 129939, at *119 (N.D. Cal. July 22, 2020); *see United States v. Thompson*, No. CR19-159-RSL, 2022 U.S. Dist. LEXIS 101558, at *3 (W.D. Wash. June 7, 2022); Reuters, *Data breach class action litigation and the changing legal landscape*, available at https://www.reuters.com/legal/legalindustry/data-breach-class-action-litigation-changing-legal-landscape-2022-06-27/. Equifax paid $380.5 million and "potentially $2 billion more . . . for credit monitoring." *In re Equifax Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1259 (11th Cir. 2021). T-Mobile recently settled its data breach litigation for $350 million. Cnet, *T-Mobile Data Breach: Are You Eligible for Money From the $350 Million Settlement?*, available at https://www.cnet.com/personal-finance/t-mobile-data-breach-are-you-eligible-for-money-from-the-350-million-settlement/ (last visited August 24, 2022).

While cases are unique and class sizes vary, Plaintiff adequately alleged that thousands of people were impacted and that the aggregate amount in controversy is well over $5,000,000. Compl., ECF No. 1, ¶ 11. The case law, and past data breach settlements, support these calculations. Defendant fails to raise any dispute as to the amount of people affected or the amount in controversy.

2. Even if not established, jurisdictional discovery will resolve the issue

Plaintiff requests permission to conduct jurisdictional discovery in the event that this Court finds that he has not made the required prima facie showing.

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

District courts have significant leeway in deciding whether to grant jurisdictional discovery. *Barantsevich v. VTB Bank*, 954 F. Supp. 2d 972, 996 (2013). In the Ninth Circuit, jurisdictional discovery should "ordinarily be granted where pertinent facts bearing on the question of jurisdiction are controverted or where a more satisfactory showing of the facts is necessary." *Id.* The threshold for granting jurisdictional discovery is low. *Harris Rutsky & Co. Ins. Servs. Inc. v. Bell & Clements Ltd.*, 328 F.3d 1122, 1135 (2003). (Where discovery might demonstrate facts to constitute jurisdiction, "we have remanded in just such a situation.").

Here, thousands of putative class members' PII was leaked. Compl., ECF No. 1, ¶¶ 26, 27. Until some discovery is conducted, Defendants are the only parties who can ascertain the number of class members. Some discovery is needed to determine the exact amount in controversy. Therefore, jurisdictional discovery is warranted.

C. Plaintiff's claims are adequately pleaded

Defendants' motion should be denied because Plaintiff properly pleaded: (1) negligence; (2) invasion of privacy; (3) breach of contract; and (4) breach of implied contract. Additionally, (5) Plaintiff has stated a claim for declaratory relief.

1. Plaintiff adequately alleged negligence

Plaintiff's negligence claim should not be dismissed because: (1) Defendants had a duty to keep private information safe from cybercriminals; (2) the data breach proximately caused injuries to Plaintiff; and (3) Plaintiff has adequately alleged damages. Also, (4) the economic loss rule does not apply.

a. Defendants had a duty to keep private information safe from criminals

Courts have consistently found that "an employer has a legal duty to exercise reasonable care to safeguard its employees' sensitive personal information stored by the employer on an internet- accessible computer system." *See*, *e.g.*, *Dittman v. UPMC*, 649 Pa. 496, 499-500, 196 A.3d 1036, 1038 (2018); *Simona Opris v. Sincera Reprod. Med.*, No. 21-3072, 2022 U.S. Dist. LEXIS 94192, at *9 (E.D. Pa. May 23,

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

2022); *Mackey v. Belden, Inc*., No. 4:21-CV-00149-JAR, 2021 U.S. Dist. LEXIS 145000, at *23 (E.D. Mo. Aug. 3, 2021) ("Other courts have reasonably held that employers embrace a duty to protect employees' PII by requiring employees to submit PII as a condition of employment."); *McKenzie v. Allconnect, Inc*., 369 F. Supp. 3d 810, 818 (E.D. Ky. 2019); *see also Brush v. Miami Beach Healthcare Grp. Ltd*., 238 F. Supp. 3d 1359, 1365 (S.D. Fla. 2017) ("It is well-established that entities that collect sensitive, private data from consumers and store that data on their networks have a duty to protect that information.") (citations omitted); *see also Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1327 (11th Cir. 2012) (finding, implicitly, that healthcare providers owe patients a duty to protect their sensitive data); *Weinberg v. Advanced Data Processing, Inc.*, 147 F. Supp. 3d 1359, 1366 (S.D. Fla. 2015) (ambulance services); *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1325 (N.D. Ga. 2019) (finding a "duty of care to safeguard the personal information in its custody"). Any arguments by Defendants otherwise, is merely a disagreement with Plaintiff's pleaded allegations, that must not be challenged on a motion to dismiss. *E.g.*, *Purvis v. Healthcare*, 563 F. Supp. 3d 1360, 1371 (N.D. Ga. 2021) (denying motion to dismiss negligence claims).

Moreover, a distinct duty of care was owed since Plaintiff was Defendants' employee and a special relationship exists. A special relationship exists between an employer and its employee. *Scialabba v. Brandise Const. Co.,* 921 P.2d 928, 930 (Nev. 1996). The rationale for imposing such liability is that:

> [S]ince the ability of one of the parties to provide for his own protection has been limited in some way by his submission to the control of the other, a duty should be imposed upon the one possessing control (and thus the power to act) to take reasonable precautions to protect the other one from assaults by third parties which, at least, could reasonably have been anticipated.

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

Id. For similar reasons, a business owes a duty to its consumers if it "has reasonable cause to anticipate such act and the probability of injury resulting therefrom." *Rockwell v. Sun Harbor Budget Suites*, 925 P.2d 1175, 1182 (Nev. 1996) (quoting *Thomas v. Bokelman*, 462 P.2d 1020, 1022 (Nev. 1970)).

Here, Defendants were, or should have been, aware of the foreseeable risks to the security of its employees' private information. Defendants thus owed a duty to reasonably protect that information. Plaintiff adequately alleged that Defendants breached that duty by failing to implement reasonable data security.

b. The data breach proximately caused injuries to Plaintiff the class

"Proximate cause is any cause which in natural and continuous sequence, unbroken by any efficient intervening cause, produces the injury complained of and without which the result would not have occurred." *Mahan v. Hafen*, 351 P.2d 617, 620 (Nev. 1960). "In Nevada, issues of negligence and proximate cause are usually factual issues to be determined by the trier of fact." *Frances v. Plaza Pac. Equities, Inc.*, 847 P.2d 722, 724 (Nev. 1993). "A negligent defendant is responsible for all foreseeable consequences proximately caused by his or her negligent act." *Taylor v. Silva*, 615 P.2d 970, 971 (Nev. 1980).

As discussed above, Plaintiff plausibly alleged that he suffered from Defendants' actions, including by the risk of harm and cognizable damages. *Anthem II*, 2016 WL 3029783, at *15; *In re Facebook Privacy Litig.*, 572 Fed. Appx. at 494. These harms, including the loss of value of PII, the risk of identity theft, and lost time, were *directly* caused by Defendants' failure to secure its employees' data.

Furthermore, Defendants' delays in notifying Plaintiff proximately increased the harm that may have been preventable or mitigated had he been timely notified. *In re Ambry Genetics Data Breach Litig.*, No. SACV 20-00791-CJC (KESx), 2021 U.S. Dist. LEXIS 204358, *13 (C.D. Cal. Oct. 18, 2021); *Anthem I,* 162 F. Supp. 3d at 987. Here, Defendants experienced the data breach in or around August 2021 but

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

did not notify the impacted victims until May 2022. Compl. ECF No. 1, ¶¶ 2, 4. Plaintiff has suffered and will continue to suffer damages as discussed above. *Id.* at ¶ 35. Defendants fail to show why these harms are not proximately caused by its breach of its duty of care.

c. Plaintiff has adequately alleged damages

As discussed above, Plaintiff plausibly pleaded a substantial risk of identity theft or fraud, a loss of value of his PII, and out-of-pocket monitoring costs, lost time, invasion of privacy, and other mental and emotional harms. All of this was exasperated by Defendants' failure to timely notify Plaintiff of the breach.

Courts have repeatedly found such harms to satisfy the damages element for a negligence claim in data breach cases. *Dittman v. UPMC*, 649 Pa. 496, 196 A.3d 1036 (2018) (employees affected by data breach properly stated a negligence claim); *Simona Opris v. Sincera Reprod. Med.*, No. 21-3072, 2022 U.S. Dist. LEXIS 94192, at *19 (E.D. Pa. May 23, 2022) ("[M]itigation damages, such as those allegedly incurred by Plaintiffs in purchasing credit and identity theft monitoring services, are a sufficient form of damages for a negligence claim.") (compiling cases); *Anthem II*, No. 15-02617, 2016 WL 3029783, at *25 ("[A] growing number of courts now recognize that individuals may be able to recover [c]onsequential [o]ut of [p]ocket [e]xpenses that are incurred because of a data breach, including for time spent reviewing one's credit accounts.").

Defendants' reliance on *Pruchnicki v. Envision Healthcare Corp.*, 439 F. Supp. 3d 1226 (D. Nev. 2020) is mistaken. In that case, unlike here, the plaintiff only alleged lost time, emotional distress, and the "diminution in value of personal and financial information." *Id.* As discussed, Plaintiff pleaded a substantial risk of identity theft or fraud, a loss of value of his PII, and out-of-pocket monitoring costs, in addition to lost time. *In re Netgain Tech., LLC, Consumer Data Breach Litig.*, No.

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

21-cv-1210 (SRN/LIB), 2022 U.S. Dist. LEXIS 98342, at *40 n.5 (D. Minn. June 2, 2022) (distinguishing *Pruchnicki*).

Defendants' reliance on *Corona v. Sony Pictures Entm't, Inc.*, No. 14-CV-09600 RGK (Ex), 2015 U.S. Dist. LEXIS 85865, at *11 (C.D. Cal. June 15, 2015) is curious since the motion to dismiss was *denied* in that case. *Id.* ("As to the risk of identity theft, it is reasonable to infer that the data breach and resulting publication of Plaintiffs' PII has drastically increased their risk of identify theft, relative to both the time period before the breach, as well as to the risk born by the general public."). *Corona* therefore supports Plaintiff's position.

Numerous courts in this Circuit have recognized that time and money spent mitigating the effects of a data breach constitute damages. *See, e.g., Huynh v. Quora, Inc.*, 508 F. Supp. 3d 633, 650 (N.D. Cal. 2020) (compiling cases); *Anthem II*, No. 15-MD-2627-LHK, 2016 WL 3029783, at *26; *Zappos*, 108 F. Supp. 3d 949, 961 (D. Nev. 2015) ("[O]nce a third party misuses a person's personal information, there is clearly an injury that can be compensated with money damages."); *Stasi*, 501 F. Supp. 3d at 918 ("It is reasonable to infer that upon receiving notice of the breach," plaintiffs would respond by ensuring that "they had not, and would not, become victims of identity theft."); *see also Castillo*, 2016 WL 9280242 at *4 (finding cognizable injury where plaintiffs purchased identity protection services "because they wanted greater protection than that offered by [Defendant]"). Plaintiff has thus sufficiently alleged damages.

d. The economic loss rule does not bar the negligence claim

The economic loss rule is a judge-made limitation wherein unintentional tort damages are barred when a plaintiff seeks recovery of "purely economic losses." *Terracon Consultants Western, Inc. v. Mandalay Resort Group*, 206 F.3d 81, 86 (Nev. 2009). The scope of the rule is limited; "[p]urely economic loss is generally defined as the loss of the benefit of the user's bargain . . . including . . . pecuniary

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

damage for inadequate value, the cost of repair and replacement of the defective product, or consequent loss of profits, without any claim of personal injury or damage to other property." *Calloway v. City of Reno*, 993 P.2d 1259, 1263 (Nev. 2000), *overruled on other grounds*, 89 P.3d 31 (Nev. 2004).

First, the doctrine does not apply since Plaintiff sustained non-economic damages. Where a plaintiff alleges both economic and non-economic losses, the doctrine is inapplicable. For example, in *Lopez*, the Nevada Supreme Court held the doctrine inapplicable in a payment dispute between an attorney and a chiropractor because the damages also included non-economic damages for lost time and reputational harm. *Lopez v. Corral*, Nos. 51541, 51972, 2010 Nev. LEXIS 69, at *10 (Dec. 20, 2010); *Huynh v. Quora, Inc*., 508 F. Supp. 3d 633, 654 (N.D. Cal. 2020) ("the economic loss rule did not bar Plaintiff's negligence claim because she alleged loss of time as a harm, meaning she had not alleged pure economic loss.").

For this reason, numerous courts recognize that in the data breach context, claims to recoup the value of lost time are not barred under the economic loss doctrine. *See In re Solara*, 2020 WL 2214152 at *45 (interpreting California law); *Stasi*, 501 F. Supp. 3d at 912-14 (same); *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1039-40 (N.D. Cal. 2019) (same); *Flores-Mendez v. Zoosk, Inc.*, No. 20-cv-04929-WHA, 2021 WL 308543, at *3 (N.D. Cal. Jan. 30, 2021) (same); *In re Netgain Tech. , LLC , Consumer Data Breach Litig.*, No. 21-cv-1210 (SRN/LIB), 2022 U.S. Dist. LEXIS 98342, *24 (D. Minn. June 2, 2022).

Here, Plaintiff's damages include both economic and non-economic losses: damages to Plaintiff's psyche, anxiety, emotional distress, lost time, and loss of privacy, that he suffered from Defendants' actions. Compl., ECF No. 1, ¶ 34. Plaintiff suffered an impairment of their PII, akin to the reputation and business harms in *Lopez*. 2010 WL 5541115 at *3-4. Accordingly, the economic loss doctrine is inapplicable in this case.

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

Second, the economic loss doctrine does not apply where the parties have a "special relationship, which is an exception to the economic loss doctrine." *Huynh v. Quora, Inc.*, 508 F. Supp. 3d 633, 654 (N.D. Cal. 2020); *see Lopez* at *3-4 ("'courts have made exceptions [to the economic loss doctrine] to allow such recovery in certain categories of cases, such as negligent misrepresentation and professional negligence actions'") (citation omitted). Courts have thus recognized a "special relationship" and resulting exception to the economic loss rule in data breach litigation arising from the obligation to protect private information. *See In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1172 (D. Minn. 2014); *In re Equifax*, 362 F. Supp. 3d at 1321.

Here, as noted above, the Nevada Supreme Court has recognized employee-employer as special relationships for negligence purposes. *Scialabba*, 921 P.2d at 930. When individuals entrust private information to their employers, they must trust the employer to store the data securely. The parties do not deal on equal terms. So, a special relationship exists and the doctrine is not applicable.

Third, as a judicially created doctrine, courts acknowledge that the policy considerations behind the rule are inapplicable in data security and privacy cases. *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F.Supp.3d 447, 475 (D. Md. 2020) ("data security breach cases do not fit neatly into the paradigm of the cases that led to the adoption of the economic loss doctrine.").

> The rationale for the economic loss doctrine stems from its origins in products liability. Tort law establishes that a product manufacturer has the responsibility of ensuring that the product does not physically harm its user. When the product only injures itself, however, principles of tort law are not implicated. Instead, contract law provides the remedy.

Mandalay Resort Grp. v. Terracon Consultants W., Inc., No. 2:04-CV-1488-RCJ-PAL, 2006 WL 8441952, at *2 (D. Nev. Feb. 21, 2006); *accord Lopez* at *4 ("Corral does not have a contract-law remedy against Lopez, and therefore, the policy

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

considerations behind the economic loss doctrine are inapplicable."). Unlike a product liability case in which a defective product injures only itself, Defendants' failure to secure PII has and will continue to cause harm for years to come. Such harm is precisely what tort law is intended to correct.

Finally, the economic-loss doctrine is inapplicable when the "nature of the claims" are in tort, and not in contact—even when a breach of contract claim is alleged. *Lopez v. Javier Corral, D.C., 367 P.3d 745*, 2010 WL 5541115, at *3-4 (Nev. Dec. 20, 2010). Where the harms included allegations that sound in tort, "the policy considerations behind the economic loss doctrine are inapplicable." *Lombino v. Bank of America, N.A.*, 797 F. Supp. 2d 1078, 1082 (D. Nev. 2011); *In re Equifax, Inc.*, 362 F. Supp. 3d 1295, 1321 (N.D. Ga. 2019) ("Therefore, since an independent duty existed [outside of a contractual obligation] the economic loss rule does not apply."). Here, the nature of Plaintiff's claims arise from Defendants' breach of an independent duty to secure Plaintiff's information. The doctrine does not apply.

2. Plaintiff adequately alleged his claims for invasion of privacy

There are four kinds of "invasion of privacy" actions in Nevada. *Franchise Tax Bd. of Cal. v. Hyatt*, 133 Nev. Adv. Rep. 57 (Nev. 2017). "[I]ntrusion upon seclusion and public disclosure of private facts" are at issue in this case. *See Id.* "To recover for the tort of intrusion, a plaintiff must prove the following elements: 1) an intentional intrusion (physical or otherwise); 2) on the solitude or seclusion of another; 3) that would be highly offensive to a reasonable person." *PETA v. Bobby Berosini, Ltd.*, 111 Nev. 615, 630 (Nev. 1995) *overruled on other grounds by City of Las Vegas Downtown Redev. Agency v. Hecht*, 113 Nev. 644, 650 (1997).For public disclosure of a private fact, such a disclosure must be "offensive and objectionable to a reasonable person of ordinary sensibilities." *Id.*

Defendants' motion should be denied because Plaintiff's medical information was disclosed. "Courts have refused to dismiss invasion of privacy claims at the

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

motion to dismiss stage where, as here, a data breach involved medical information, because the disclosure of such information is more likely to constitute an 'egregious breach of the social norms' that is 'highly offensive.'" *In re Ambry Genetics Data Breach Litig.*, No. SACV 20-00791-CJC (KESx), 2021 U.S. Dist. LEXIS 204358, at *17-18 (C.D. Cal. Oct. 18, 2021) (citing cases); *Doe v. Beard*, 63 F. Supp. 3d 1159, 1170 (C.D. Cal. 2014) (the disclosure involved medical information and, thus, was subject to a 'lower threshold' for 'egregious violations of social norms.'"); *see also In re Facebook Inc. Internet Tracking Litig.*, 956 F.3d 589, 606 (9th Cir. 2020) (allegations of Facebook's tracking and data collection practices met the "reasonable expectation of privacy" and "highly offensive" elements for invasion of privacy claim). Here, information stolen in the breach included Plaintiff's medical information, as well as his social security number and other highly personal information. *See* Compl., ECF No. 1, ¶ 5. A reasonable person would find the exposure of such information to be highly offensive. *Id.* at ¶¶ 59-62. Defendants' conduct was highly offensive. Defendants' motion should be denied.

3. Plaintiff adequately alleged a breach of contract claim

Plaintiff adequately pleaded that Defendants breached the contract when they failed to maintain adequate security measures to protect Plaintiff's PII.

The case law overwhelmingly supports that a breach of contract claim exists when a company fails to protect its consumers' or employees' private information, resulting in a data breach. *See*, *e.g.*, *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, No. 3:19-cv-2284-H-KSC, 2020 U.S. Dist. LEXIS 80736, at *16 (S.D. Cal. May 7, 2020) (denying motion to dismiss a breach of implied contract and breach of express contract claims in data breach action); *In re Marriott Int'l, Inc.*, 440 F. Supp. 3d 447, 485 (D. Md. 2020) (denying motion to dismiss claims for breach of express contract and implied contract under various state laws); *Rudolph v. Hudson's Bay Co.*, No. 18-cv-8472 (PKC), 2019 U.S. Dist. LEXIS 77665, at *35

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

(S.D.N.Y. May 7, 2019) (denying motion to dismiss a claim for breach of implied contract in data breach case); *In re Brinker Data Incident Litig.*, No. 3:18-cv-686-J-32MCR, 2020 WL 691848, at *4 (M.D. Fla. Jan. 27, 2020) (upholding breach of implied contract claim and stating: "The majority of federal courts have held that the existence of an implied contract to safeguard customers' data could reasonably be found to exist between a merchant and customer when a customer uses a payment card to purchase goods and services); *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 159 (1st Cir. 2011) (a reasonable jury could find that an implied contract existed that company would reasonably protect its customers' credit card information); *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 531 (N.D. Ill. 2011) (denying motion to dismiss claim for breach of an implied contract in case involving a credit card security issue); C*astillo v. Seagate Tech., LLC*, No. 16-cv-01958-RS, 2016 U.S. Dist. LEXIS 187428, at *29 (N.D. Cal. Sep. 14, 2016) ("the mandatory receipt of . . . sensitive personal information [implies] the recipient's assent to protect the information sufficiently.").

Here, Plaintiff properly pleaded that a contract existed wherein Defendant promised to safeguard his data. *See* Compl., ECF No. 1, ¶¶ 63-72. As a condition of employment, Plaintiff was required to provide his personal information to Defendants, and "[a] meeting of the minds occurred, as Plaintiff and Class Members agreed, among other things, to provide their Private Information in exchange for Defendants' agreement to protect the confidentiality of that Private Information." *Id.* at ¶ 66. Defendants fail to cite *any* on-point case.

In addition, "whether a contract exists is [a question] of fact." *Certified Fire Prot. Inc. v. Precision Constr.*, 283 P.3d 250, 255 (2012). Here, Defendants' attempts to argue that a contract did not exist is improper at this stage. A reasonable jury could find that an agreement was entered into by the parties and that Defendants breached that agreement by failing to keep Plaintiff's private information secure.

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

4. Plaintiff has adequately alleged a claim for breach of implied contract

"Where the terms of a contract are literally complied with but one party to the contract deliberately contravenes the intention and spirit of the contract, that party can incur liability for breach of the implied covenant of good faith and fair dealing." *Hilton Hotels Corp. v. Butch Lewis Prods., Inc.*, 107 Nev. 226, 232 (1991). The elements of breach of implied contract include a valid contract, breach, and damages. *Mizrahi v. Wells Fargo Home Mortg.,* 2010 WL 2521742, at *3 (D. Nev. 2010).

Courts have upheld implied contract claims in data breach cases. "[T]he mandatory receipt of Social Security numbers or other sensitive personal information [implies] the recipient's assent to protect the information sufficiently." *Castillo*, No. 16-cv-01958-RS, 2016 U.S. Dist. LEXIS 187428, at *29 (citing *Target*, 66 F. Supp. 3d at 1176 (finding "an implied contract in which Plaintiffs agreed to use their credit or debit cards to purchase goods at Target and Target agreed to safeguard Plaintiffs' personal and financial information")); *see Rudolph v. Hudson's Bay Co.*, 2019 U.S. Dist. LEXIS 77665, 2019 WL 2023713, at *11 (S.D.N.Y. May 7, 2019) (citing cases); *In re GE/CBPS Data Breach Litig.*, 2021 U.S. Dist. LEXIS 146020, 2021 WL 3406374, at *12 (S.D.N.Y. Aug. 4, 2021) (employees in a data breach case sufficiently stated a claim for breach of implied contract).

Here, "Defendants agreed to reasonably protect such information. . . . Plaintiff . . . reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards." Compl., ECF No. 1, ¶¶ 76-77. Plaintiff adequately pleaded his claim.

Plaintiff also adequately alleged damages for his breach of implied contract claim. "The dissemination of one's personal information can satisfy the damages element of a breach of contract claim." *Solara*., 2020 WL 2214152, at *5; *In re Google Assistant Priv. Litig*., 457 F. Supp. 3d 797, 834 (N.D. Cal. 2020) (plaintiff may seek damages for "the detriment caused by the breach," including nominal

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

damages for such harm); *Georges Tannoury, MD, PC v. Stacey Kokopelli Med., P.C.*, 130 Nev. 1181, 2014 WL 1270582, at *1 n.2 (2014) (a plaintiff is entitled to nominal damages upon a breach of contract, even where they cannot prove actual damages); *Gramanz v. T–Shirts & Souvenirs, Inc*., 894 P.2d 342, 347 (Nev. 1995).

Here, at minimum, Plaintiff is entitled to nominal damages. Compl., ECF No. 1, ¶ 88. Plaintiff alleged legally cognizable damages for his contract claims. Plaintiff's breach of implied contract claim is properly pleaded.

5. Plaintiff has stated a claim for declaratory and injunctive relief

Plaintiff alleged a claim for declaratory and injunctive relief under 28 U.S.C. § 2201(a). *See, e.g., In re Arby's Rest. Grp. Inc. Litig.*, No. 1:17-cv-0514-AT, 2018 U.S. Dist. LEXIS 131140, 2018 WL 2128441, at *15 (N.D. Ga. Mar. 5, 2018) (data breach case; the claim for declaratory judgment survived); *Gordon v. Chipotle Mexican Grill, Inc.,* 344 F. Supp. 3d 1231, 1252 (D. Colo. 2018) (injunctive relief was available to address "insufficiently secured computer systems"); *Adkins v. Facebook, Inc.*, 424 F. Supp. 3d 686, 698-99 (N.D. Cal. 2019) (allowing class to pursue injunctive relief "to promptly correct any problems or issues detected by third party auditors"). Here, Plaintiff alleged that his private information is still in Defendants' inadequate system. Plaintiff properly stated a claim for declaratory and injunctive relief, independent of his other claims.

V. Conclusion

Plaintiff respectfully requests that this Court deny Defendants' motion.

///

///

///

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123

However, out of an abundance of caution, Plaintiff specifically requests leave to amend to address any pleading defects in his complaint.

Dated this ___ day of August 2022.

Respectfully submitted,

KIND LAW

/s/ Michael Kind
Michael Kind, Esq.
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123
Attorney for Plaintiff Jehu Bryant

KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123